Amendments to the Specification

Please delete paragraph 34 beginning on page 5, line 29 in its entirety.

Please replace the paragraph beginning at page 6, line 1, with the following rewritten paragraph:

[107] Figure ~~21~~ 20 is a flowchart showing the steps of an illustrative process for processing a URL received in a forwarding server using the apparatus of Figure 19.

Please replace the paragraph beginning at page 6, line 3, with the following rewritten paragraph:

[108] Figure ~~22~~ 21 is a block schematic diagram of an embodiment of the invention in which a metrics server located at an application service provider site receives content from several publishers and requests for content from the publisher's server and delivers encrypted content to a viewer located in a user browser.

Please replace the paragraph beginning at page 6, line 7, with the following rewritten paragraph:

[109] Figure ~~23~~ 22 is a block schematic diagram of still another embodiment in which encrypted content data is stored locally on a user's computer and is decrypted and displayed in a secure viewer using decryption keys that are downloaded from a networked server.

Please replace the paragraph beginning at page 6, line 11, with the following rewritten paragraph:

[110] Figure ~~24~~ 23 is a block schematic diagram of yet another embodiment in which encrypted content data, a secure viewer and encrypted decryption keys are stored locally on a user's computer.

Please replace the paragraph beginning at page 24, line 21, with the following rewritten paragraph:

[99] In accordance with another aspect of the invention, in the distributed mode, a client can "forward" a content document to one or more recipient e-mail addresses, including addressees who are not part of the client's corporate network. This forwarding process allows the recipients to access the specified content without losing the content protection. It also allows the inventive distribution system to track usage activity of recipient users in the same fashion as previously-registered users. This process is illustrated in Figures 19~~, 20~~ and ~~21~~ 20. An overall view of the process is illustrated in Figure 19. The steps ~~in preparing the e-mail are shown in Figure 20 and the steps~~ in receiving and processing the content document identification information from the e-mail recipient are shown in Figure ~~21~~ 20.

Please replace the paragraph beginning at page 25, line 1, with the following rewritten paragraph:

[100] The process begins ~~in step 2000 and proceeds to step 2002 where~~ when a user logged into a customer site server (for example server 1204, Figure 12) at a customer site 1900 uses the metrics viewer operating in his browser to send an e-mail to another user in order to "forward" a selected content document. The metrics viewer communicates to the customer site server 1204 to prepare an email with a link to the original publisher site 1902. ~~In step 2002, the~~ The customer site server 1204 uses a sender ID generator 1904 to generate a sender ID. Generally, the sender ID would be a text string identifying the sender and the sender's corporate network. Next, ~~in step 2004,~~ the server 1204 uses a recipient ID generator 1906 to generate a recipient ID. Generally, the recipient ID would be a text string identifying the recipient and the recipient's corporate network.

Please replace the paragraph beginning at page 25, line 12, with the following rewritten paragraph:

[101] Then, ~~in step 2006,~~ the server 1204 uses a document ID generator 1908 to generate an ID identifying the content document that will be forwarded. This content ID might be the document name or URL. ~~In step 2008, a~~ A concatentator 1910 concatenates the three IDs and~~, in step 2010,~~ the ID information is encrypted with an

encryptor 1912. In one embodiment, this latter encryption might be RSA public key encryption using the public key of the publisher site that originated the content document. The encrypted ID string is then inserted into a URL that appears as a link when the e-mail arrives in the recipient's e-mail program or browser ~~as set forth in step 2012. The process then finishes in step 2014.~~ Subsequently, the e-mail 1918 is sent to the recipient.

Please replace the paragraph beginning at page 25, line 26, with the following rewritten paragraph:

[102] When the recipient clicks on the link to the publisher in the e-mail, a supported browser is opened and the browser navigates to a "forwarding" metrics server in the publisher's site. This server might be server 1206 in publisher site 1200 as shown in Figure 12. During this process, the URL in the e-mail is sent to the server and processed as set forth in Figure ~~21~~ 20. The server then downloads the metrics viewer described previously into the recipient's browser and launches the viewer as hosted by the server. The recipient then logs into the server 1206 and registers in the fashion described above.

Please replace the paragraph beginning at page 26, line 21, with the following rewritten paragraph:

[105] A block schematic diagram of another embodiment of the inventive content distribution system is shown in Figure ~~22~~ 21. In this embodiment, the metrics server 2206 is hosted by a third party, called an application service provider 2204. One or more publishers, 2330, 2232, periodically upload new content to the application service provider 2204 using conventional means, such as CDs or network transfers, as indicated schematically by arrows 2226 and 2228, respectively. Content received from the publishers at the application service provider 2204 is processed by a publishing tool 2224 located at the application service provider location 2204 in order to generate encrypted content. The encrypted content is stored in databases 2218 at the application service provider location 2204, as indicated schematically by arrow 2222.

Please replace the paragraph beginning at page 27, line 1, with the following rewritten paragraph:

[106] In this embodiment, a document identifier is computed by the metrics server 2206 at the application service provider site 2204 from the encrypted content and stored with a decryption key. Users 2200 and 2202 interested in receiving the content log into the metrics server 2206 at the application service provider site 2204 as indicated schematically by arrows 2208 and 2210, respectively. As indicated schematically by arrow 2214, the metrics server 2206 retrieves user information and profiles from the metrics user database 2212 located at the application service provider site 2204 and uses this information to log in the users as described above. During the login procedure, secure content viewer software (not shown in Figure ~~22~~ 21) is downloaded into the user's local browser. In order to access the content, the content viewer requests a selected document from the application service provider server 2206 by referring to a document name or URL. As indicated schematically by arrow 2216, the server 2206 retrieves the document from the content database 2218 and forwards it to the viewer in encrypted form. The viewer then computes a document identifier from the encrypted document content and uses the identifier to request a key from the server 2206 in order to decrypt the document. The key is forwarded from the server 2206 to the viewer, which then decrypts the document and displays it in the viewer.

Please replace the paragraph beginning at page 27, line 21, with the following rewritten paragraph:

[108] Still another embodiment is illustrated in Figure ~~23~~ 22. In this embodiment, a user can elect to store encrypted content in a database 2314 located on his or her computer 2304. For example, the content may be delivered from a publisher site 2302 by conventional means, such as CDs or DVDs. In order to view the content, the user must log in to a metrics key server 2316 located at the publisher's site 2302 or another central location using a conventional browser 2304, as indicated schematically by arrow 2308. During the login procedure, the secure content viewer software 2306 is downloaded over the network into the user's browser 2306 as indicated schematically by arrow 2310. In response to information from the user identifying a document, the

content viewer 2306 reads the encrypted content from the local database 2314, and computes a document identifier from the encrypted content in a manner previously discussed. The viewer 2306 then sends the document identifier to the key server 2316 in order to retrieve decryption keys from the key database 2318. The decryption keys are then used to decrypt the encrypted content in the secure viewer software 2306.

Please replace the paragraph beginning at page 28, line 5, with the following rewritten paragraph:

[109] Still another embodiment is illustrated in Figure ~~24~~ 23 in which encrypted content data is stored in a local database 2410 on the user's computer 2400. The secure content viewer software 2404 is also stored on the user's computer 2400. Decryption keys along with document identifiers may also be stored in a key database 2412 in encrypted form on the user's computer. For example, the decryption keys may be encrypted with a key that is embedded in the viewer software 2404. Alternatively, the decryption keys may be retrieved from a networked key server (not shown in Figure 24) as described in the previous embodiment. In response to information from the user identifying a document, the content viewer 2404 reads the encrypted content from the local database 2410, and computes a document identifier from the encrypted content in a manner previously discussed. The viewer 2404 then retrieves an encrypted decryption key from the local key database 2412. The decryption keys are then used to decrypt the encrypted content in the secure viewer software 2404.